IEEE Std 1609.2-2016 Guidance Note 8: Generation Time

William Whyte, Security Innovation

Version 0.1, 2016-08-16

1 Introduction

This note identifies an area in IEEE Std 1609.2-2016 that may cause confusion to implementers and to specifiers of Secure Data Exchange Entities (SDEEs, i.e. any entity that makes use of WAVE Security Services as defined in 1609.2). The note clarifies the relevant text, which is ambiguous as to whether or not a signed SPDU's generation time is required by the security services when verifying that signed SPDU. The clarification is that the generation time **is** required.

2 Summary of issue

1609.2 clause 5.2.3.2.2 states the following.

A signed SPDU contains the following information elements that are used when determining validity:

- Required:
  - Identifier of signing certificate
  - Associated PSID
  - One of: Encapsulated payload or hash of external payload
- Optional:
  - Generation location (see 5.2.2)
  - Generation time (see 5.2.2)
  - Expiry time

It then states that the signed SPDU is consistent with the signing certificate if "all the following hold":

- The signing certificate is an authorization certificate, i.e., it contains application permissions.
- The stated generation location is consistent within the geographic region indicated in the certificate, i.e., one of the following conditions holds:
  - Either the certificate is valid worldwide.
  - Or the certificate has a geographic restriction, the SDEE specification states that the signed SPDU contains a generation location, and the generation location is within the geographic restriction.
  - Or the certificate has a geographic restriction but the SDEE specification states that the SPDU generation location is not used for consistency checks. (This can be stated using the 1609.2 security profile specified in Annex C.)

— The stated generation time is within the validity period of the certificate.

— The expiry time, if present, is within the validity period of the certificate.

— The PSID that appears in the security envelope of the signed SPDU appears in the *appPermissions* field of the certificate.

— The public key in or associated with the certificate can be used to cryptographically verify the signature on the PDU.

The **possible cause of confusion** is that the first quoted section says that generation time is optional, but the second quoted section is not written as if it is optional. In fact, the second section uses the phrasing "The expiry time, if present", in contrast to the phrasing "The stated generation time." This implies that generation time is required. This might lead a reader to think the standard is contradicting itself.

The **actual requirement intended to be stated in 1609.2** is that the Secure Data Service must be passed the generation time when verifying. This may come from the 1609.2 security headers or from elsewhere.

The **proposed resolution** is to change the relevant bullet point in the second quoted section to read:

— The stated generation time <u>(which is obtained from the signed SPDU if it is present there, and if not is provided to the SDS by the SDEE)</u> is within the validity period of the certificate.